DEU

PX-3309

Bewegliche Wireless Netzwerk
IP-Kamera



Installationsanleitung

7links™

Bewegliche Wireless Netzwerk

IP-Kamera

DEU

INHALTSVERZEICHNIS

EINLEITUNG

INSTALLATIONSANLEITUNG FÜR EINSTEIGER

7Links™

ANHANG

EINLEITUNG

IHRE NEUE IP-KAMERA

Sehr geehrte Kunden,

vielen Dank für den Kauf dieser Wireless Netzwerk IP Kamera, einer leistungsstarken kabellosen Netzwerkkamera für Bilder mit hoher Qualität und mit Audio vor Ort via Internetverbindung. Dank der Schwenk-/Neigungsfunktionen kann die Kamera für die Fernüberwachung an allen Orten gesteuert werden. An die GPIO-Anschlüsse können verschiedene externe Geräte angeschlossen werden. Diese Kamera kann leicht und schnell als ein unabhängiges System innerhalb Ihrer Anwendungsumgebung installiert werden und ist so die ideale Fernüberwachung.
Bitte beachten Sie die folgenden Hinweise zum Aufbau der Bedienungsanleitung und lesen Sie alle Kapitel sorgfälltig durch, damit Sie Ihre neue Kamera optimal einsetzen können.

VERWENDUNG DIESER INSTALLATIONSANLEITUNG

Dies ist lediglich eine Installationsanleitung. Die ausführliche Anleitung mit einer Beschreibung des vollen Funktionsumfangs Ihrer neuen IP-Kamera finden Sie im Internet auf www.pearl.de. Klicken Sie auf der Seite links auf **SUPPORT (Treiber & Co.)** unter der Überschrift **Service**. Geben Sie dann die Artikelnummer PX-3309 in das Suchfeld ein und klicken Sie auf **OK**. Zum Öffnen der Bedienungsanleitung benötigen Sie eine aktuelle Version des Adobe Acrobat Reader den Sie kostenfrei auf der Homepage des Anbieters herunterladen können.

Verwendete Symbole

	Dieses Symbol steht für mögliche Gefahren und wichtige Informationen im Umgang mit diesem Produkt. Es wird immer dann verwendet, wenn der Anwender eindringlich auf etwas hingewiesen werden soll.
	Dieses Symbol steht für nützliche Hinweise und Informationen, die im Umgang mit dem Produkt helfen sollen „Klippen zu umschiffen“ und „Hürden zu nehmen“.
	Dieses Symbol wird für beispielhafte Anwendungen und Erläuterungen verwendet, die oft komplexe Vorgehensweisen veranschaulichen und begreiflich machen sollen.
	Dieses Symbol wird oftmals hinter Fachbegriffen zu finden sein, zu denen weitere Erläuterungen im Glossar zu finden sind. Das Glossar soll dabei helfen, diese Fachbegriffe für den Laien verständlich zu machen und in einen Zusammenhang zu rücken.

Verwendete Textmittel

GROSSBUCHSTABEN	Großbuchstaben werden immer dann verwendet, wenn es gilt Tasten, Anschluss- oder andere Produkt-Beschriftungen kenntlich zu machen.
Fettschrift	Fettschrift wird immer dann eingesetzt, wenn Menüpunkte oder genau so bezeichnete Ausdrücke in der Software des Produktes verwendet werden.
1. Aufzählungen 2. Aufzählungen 3. Aufzählungen	Aufzählungen werden immer dann verwendet, wenn der Anwender eine bestimmte Reihenfolge von Schritten befolgen soll, oder die Merkmale des Produktes beziffert werden sollen.

Gliederung

Diese Anleitung ist untergliedert in vier grundlegende Bestandteile:

Einleitung	Erläuterungen zur Nutzung dieser Anleitung, Wichtige Hinweise zur Sicherheit im Umgang mit dem Produkt, Übersicht über das Produkt
Installationsanleitung	Detaillierte Anleitung zur Installation und Inbetriebnahme der IP-Kamera und zur grundlegenden Konfiguration unter Berücksichtigung der Anwendungsumgebung.
Anhang	Troubleshooting (Problemlösungen), Glossar, Konformitätserklärung

WICHTIGE HINWEISE ZU BEGINN

Sicherheit & Gewährleistung

- Diese Bedienungsanleitung dient dazu, Sie mit der Funktionsweise dieses Produktes vertraut zu machen. Bewahren Sie diese Anleitung daher stets gut auf, damit Sie jederzeit darauf zugreifen können.
- Sie erhalten bei Kauf dieses Produktes zwei Jahre Gewährleistung auf Defekt bei sachgemäßem Gebrauch. Bitte beachten Sie auch die allgemeinen Geschäftsbedingungen!
- Bitte verwenden Sie das Produkt nur in seiner bestimmungsgemäßen Art und Weise. Eine anderweitige Verwendung führt eventuell zu Beschädigungen am Produkt oder in der Umgebung des Produktes.
- Ein Umbauen oder Verändern des Produktes beeinträchtigt die Produktsicherheit. Achtung Verletzungsgefahr!
- Öffnen Sie das Produkt niemals eigenmächtig. Führen Sie Reparaturen nie selber aus!
- Behandeln Sie das Produkt sorgfältig. Es kann durch Stöße, Schläge oder Fall aus bereits geringer Höhe beschädigt werden.
- Halten Sie das Produkt fern von Feuchtigkeit und extremer Hitze.
- Tauchen Sie das Produkt niemals in Wasser oder andere Flüssigkeiten.

ACHTUNG
Es wird keine Haftung für Folgeschäden übernommen.
Technische Änderungen und Irrtümer vorbehalten!

Informationen zur Entsorgung von elektrischen und elektronischen Geräten

Ihr neues Produkt wurde mit größter Sorgfalt entwickelt und aus hochwertigen Komponenten gefertigt. Trotzdem muss das Produkt eines Tages entsorgt werden. Die durchgestrichene Mülltonne bedeutet, dass Ihr Produkt am Ende seiner Lebensdauer getrennt vom Hausmüll entsorgt werden muss. Bitte bringen Sie in Zukunft alle elektrischen oder elektronischen Geräte zu den eingerichteten kommunalen Sammelstellen in Ihrer Gemeinde. Diese nehmen Ihre Geräte entgegen und sorgen für eine ordnungsgemäße und umweltgerechte Verarbeitung. Dadurch verhindern Sie mögliche schädliche Auswirkungen auf Mensch und Umwelt, die sich durch unsachgemäße Handhabung von Produkten am Ende von deren Lebensdauer ergeben können. Genaue Informationen zur nächstgelegenen Sammelstelle erhalten Sie bei Ihrer Gemeinde.

Konformitätserklärung

Hiermit erklärt Pearl Agency, dass sich dieses Produkt PX-3309-675 in Übereinstimmung mit den grundlegenden Anforderungen der Richtlinie 1999/5/EG befindet.

Pearl Agency
Pearl-Str. 1-3
79426 Buggingen
Deutschland
27.01.2010

Die ausführliche Konformitätserklärung finden Sie unter www.pearl.de.

Importiert von:
PEARL Agency GmbH • PEARL-Straße 1-3 • D-79426 Buggingen

PRODUKTINFORMATIONEN

Die IP-Kamera bietet sowohl dem Heimanwender, als auch professionellen Nutzern eine Vielzahl an Anwendungsgebieten. Für optimalen Schutz stehen außerdem die, zum heutigen Sicherheitsstandard gehörenden, Verschlüsselungsvarianten WPA und WPA2 zur Verfügung. Mit den 802.11b/g Standards erreichen Sie Datendurchsatzraten bis zu 54 MBit/s. Die externe Antenne ermöglicht hierbei einen verlustarmen Datentransfer über weite Strecken. Unter normalen Umweltbedingungen kann die Kamera im gesamten Sendegebiet Ihres WLAN-Routers arbeiten. Für die Fernüberwachung kann die Kamera Momentaufnahmen und Videos als Emails versenden oder diese sogar auf voreingestellte FTP-Server laden.

Lieferumfang

- IP-Kamera
- WLAN-Antenne
- Netzwerkkabel (RJ45)
- Wandhalterung
- GPIO-Stecker
- Netzteil
- Software-CD
- Bedienungsanleitung

Technische Daten

- 1/4"-CMOS-Sensor (Farbe)
- Auflösung: 640 x 480 Pixel (VGA)
- Nachtsicht durch 10 IR-LEDs: bis 10 m Reichweite
- Lichtempfindlichkeit: 0,5 Lux
- Sichtfeld: horizontal 280°, vertikal 90°
- Bildfrequenzrate: max. 30 fps
- Bewegungserkennung mit automatischem Bild-Versand per E-Mail
- Integriertes Mikrofon
- Unterstützt die wichtigsten Internet- und Einwahlprotokolle: HTTP, FTP, TCP/IP, SMTP, DHCP, UDP, UPnP, DDNS, PPPoE u.a.
- WLAN: Übertragungsgeschwindigkeit bis 54 Mbit/s (IEEE 802.11g) mit WEP/WPA/WPA2-Verschlüsselung
- Integrierter Web-Server
- Maße: 100 mm x 125 mm

Systemvorraussetzungen

- **Netzwerk**
  - LAN: 10 Base-T Ethernet oder 100 Base-TX Fast Ethernet
  - WLAN: IEEE 802.11b/g.

- **Computer für Web Browser Zugriff**
  - Betriebssystem: Microsoft Windows 2000/XP/Vista/7
  - Arbeitsspeicher: 128 MB RAM
  - Auflösung: 800 x 600 oder besser
  - Browser: Microsoft Internet Explorer (8.0 oder neuer)
  - Prozessor: Intel Pentium III 800 MHz oder besser

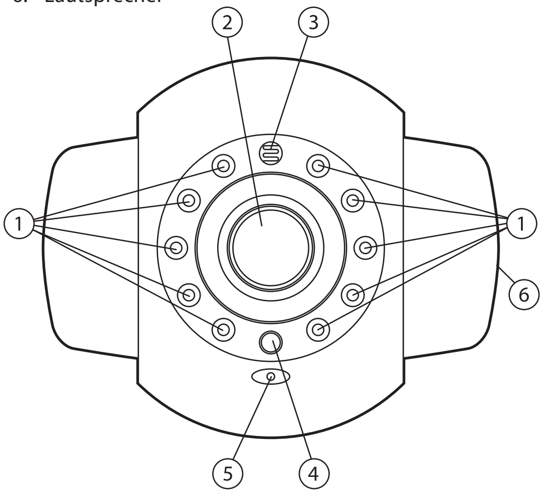
Angeschlossene Kameras	Prozessor	Arbeitsspeicher
1	Pentium III / 800 MHz	512 MB RAM
2 bis 4	Pentium 4 / 1,3 GHz	512 MB RAM
5 bis 8	Pentium 4 / 2,4 GHz	1 GB RAM
9 bis 16	Pentium 4 / 3,4 GHz	2 GB RAM

Statt eines Intel Pentium Prozessors kann jeweils auch ein AMD Prozessor mit vergleichbaren Leistungswerten verwendet werden. Die hier angegebenen Daten sind die minimal benötigten Werte. Höhere Leistungswerte erleichtern in jedem Fall die Bedienung und beschleunigen die Installation und Verwendung.

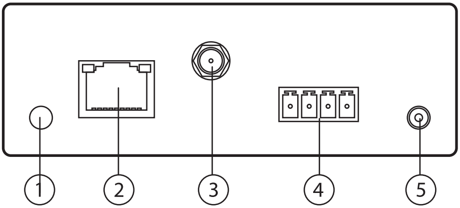
HINWEIS:
Die Software der Kamera verwendet ActiveX-Steuerelemente, verwenden Sie daher nur den Internet Explorer und keine anderen Browser wie Mozilla Firefox, Apple Safari oder Google Chrome.

Detailsansicht

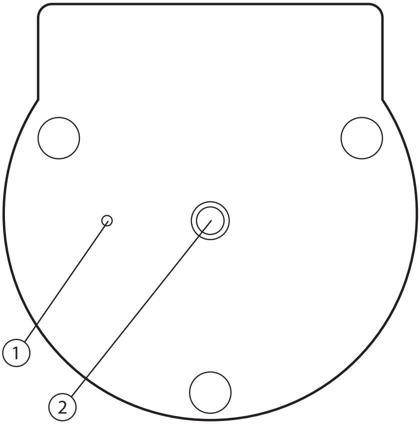
- **Vorderseite**
  1. Infrarot-LEDs
  2. Linse (CMOS Sensor mit fest integrierter Linse)
  3. Lichtsensor
  4. Netzwerk LED
  5. Mikrofon
  6. Lautsprecher



- **Rückseite**
  1. Kopfhörerausgang
  2. RJ45 Ethernet-Anschluss
  3. Antenne
  4. I/O Alarm-Anschlüsse
  5. Netzteil-Anschluss



- **Unterseite**
  1. Reset-Taste
  2. Halterungsöffnung



INSTALLATIONSANLEITUNG

VORBEREITUNG UND MONTAGE

HINWEIS:
Viele der Fachbegriffe werden im Anhang „Basiswissen Netzwerke" erläutert (ab Seite 64). Sollten dennoch Fragen bezüglich der Installation bestehen, können Sie sich gerne an unsere Service-Hotline wenden.

Produktempfehlungen
Zusätzlich zu den unbedingt notwendigen Zubehörteilen empfehlen wir Ihnen für die Erweiterung Ihres Netzwerkes und die Verwendung der Kamera folgende Artikel aus unserem Sortiment:

PE-5586	ConnecTec 10/100MBit Netzwerk-Switch 5-Port USB mit blauen LEDs
PX-6516	TP-LINK 54Mbit WLAN-USB-Dongle „TL-WN321G" USB2.0 (802.11g/b)
PE-4454	revolt Profi-Steckdosenleiste mit Netzwerkschutz

Vorbereitung

HINWEIS:
Sollten Sie sich bei den folgenden Fragen nicht sicher sein, empfehlen wir Ihnen, sich an einen Fachmann zu wenden. Eine Fehlkonfiguration der Kamera kann den Zugriff auf diese unmöglich machen.

Um eine reibungslose Installation der Kamera gewährleisten zu können, sollten Sie folgende Daten im Vorfeld recherchieren und bereithalten:

1. Die Zugangsdaten Ihres Serviceproviders (Internet-Anbieters)
2. Die IP-Adresse ↘ des Gateway-Routers ↘.
3. Wird in Ihrem Netzwerk bereits ein DHCP-Server ↘ verwendet? Wenn ja – welche Adressräume deckt dieser ab?

Ferner sollten Sie folgendes im Vorfeld beachten:

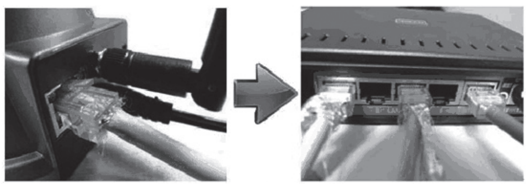
- Bei der Erstinstallation muss die Kamera direkt über Kabel mit einem Computer verbunden werden.
- Beseitigen Sie eventuelle Störquellen im Funktionsbereich Ihres WLAN-Routers. Hierzu gehören Funktelefone, Funküberwachungskameras und andere Geräte, die mit dem 2,4 GHz Band funktionieren.
- Verwenden Sie zwischen Kamera und Router kein Kabel, das länger als 25 m ist – bei ungünstigen Verhältnissen kann es sonst zu einem Spannungsabfall kommen und die Kamera kann keine Signale mehr übertragen.
- Schalten Sie zur Einbindung der Kamera in ein bestehendes Netzwerk alle Firewalls ↘, Virenscanner, MAC-Adressenfilter ↘ und Verschlüsselungen ↘ Ihres Computers aus.
- Notieren Sie sich die SSID ↘ Ihres bestehenden WLAN-Netzwerks.

HINWEIS:
Am Ende dieser Installationsanleitung finden Sie eine Checkliste zur Installation und Inbetriebname. Trennen Sie die Liste mit einer Schere heraus und verwenden Sie diese um die einzelnen Punkte abzuarbeiten.

Anschluss und Inbetriebnahme

ACHTUNG:
Beachten Sie unbedingt die Reihenfolge der nächsten Schritte und führen Sie diese genau in dieser aus.

1. Verwenden Sie das Netzwerkkabel, um die Kamera mit einem freien Ethernet-Anschluss Ihres Routers oder einem Netzwerkswitch, der an diesen angeschlosssen ist zu verbinden. Verbinden Sie dann das Netzteil mit der Stromversorgung und dem Stromanschluss der IP-Kamera.



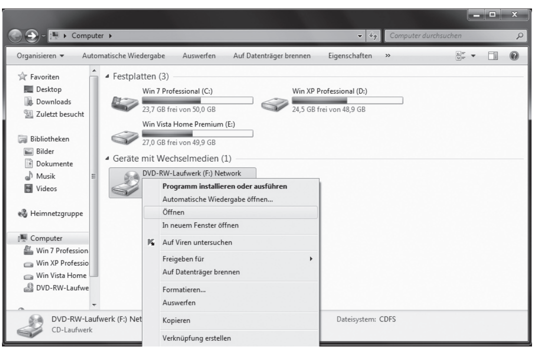
HINWEIS:
Es wird empfohlen, das Netzteil nur mit einer Mehrfachsteckdosenleiste mit integriertem Überspannungsschutz zu verbinden.

2. Starten Sie Ihren Computer und führen Sie die Softwareinstallation aus, um auf die Kamera zuzugreifen.
3. Legen Sie die mitgelieferte Software-CD in ein freies CD-/DVD-Laufwerk Ihres Computers.

4. Wählen Sie **autorun.exe ausführen**, nachdem Windows die CD erkannt hat. Gehen Sie dann zu Schritt 5.



Sollte die CD nicht automatisch erkannt werden, öffnen Sie Ihren Arbeitsplatz/Computer und wählen Sie das Laufwerk mit einem Rechtsklick aus.



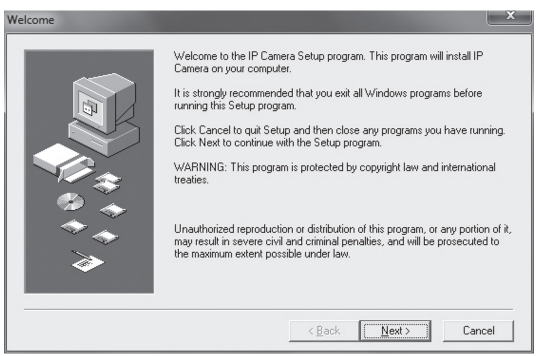
5. Wählen Sie **Explorer/Öffnen**, um den Inhalt der CD anzeigen zu lassen.



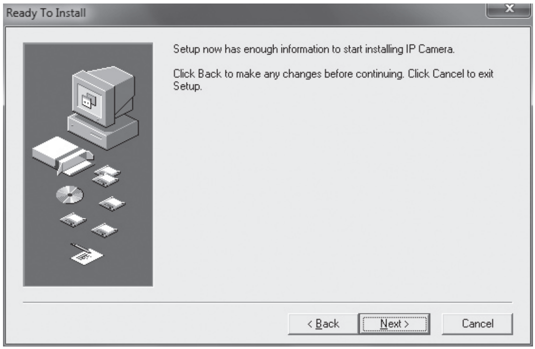
Starten Sie die Datei **IP-Finder** mit einem Doppelklick.

HINWEIS:
Nach dem Start blendet Windows die folgende Warnmeldung ein: ***Möchten Sie zulassen, dass durch das folgende Programm von einem unbekannten Herausgeber Änderungen an diesem Computer vorgenommen werden?*** *Die Installation kann nur fortgesetzt werden, wenn Sie* ***Ja*** *klicken.*

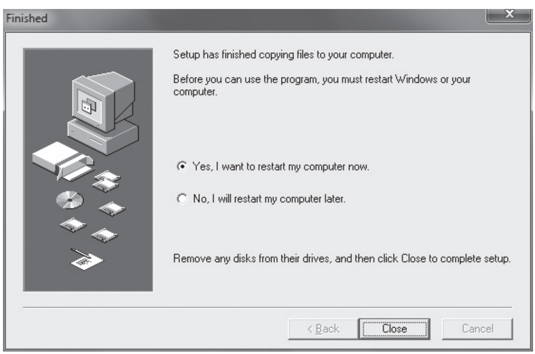
6. Folgen Sie den Anweisungen des Installationsassistenten und klicken Sie auf **Next**.



7. Bestätigen Sie im nächsten Fenster erneut mit **Next**.



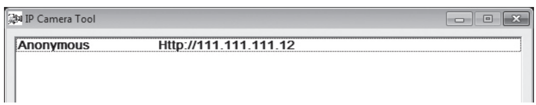
8. Wählen Sie **Yes, I want to restart my computer now** und klicken Sie auf **Close**.



9. Warten Sie bis Ihr Computer neu gestartet wurde und führen Sie das neue Programm **IP Camera Tool** auf Ihrem Desktop mit einem Doppelklick aus.



10. Werkseitig ist bei der Kamera die Adressannahme per DHCP ↘ eingestellt. Im **IPFinder**-Fenster werden Ihnen angeschlossene Kameras, sowie deren IP-Adressen ↘ angezeigt.



11. Starten Sie den Microsoft Internet Explorer.

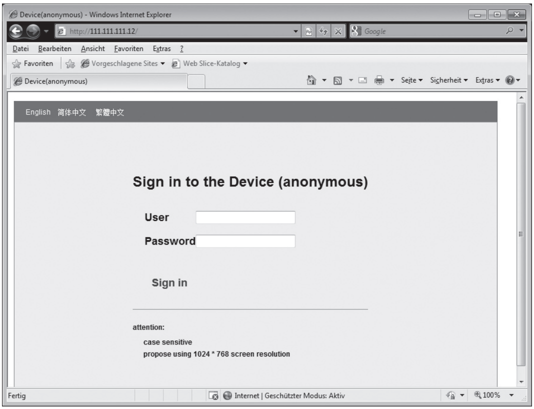
HINWEIS:
Verwenden Sie nur den Microsoft Internet Explorer für die Bedienung der Kamera. Andere Browser ↘, wie z.B. Mozilla Firefox, können die benötigten ActiveX Steuerlemente nicht darstellen.

12. Geben Sie die angezeigte IP-Adresse ↘ in die Adresszeile des Internetexplorers ein.



BEISPIEL:
Wenn die Kamera unter der IP-Adresse **168.198.0.10** angezeigt wurde muss die Eingabe im Internetexplorer **http:// 168.198.0.10** lauten.

13. Im Explorer erscheint jetzt die Online-Steuerung der IP-Kamera. Die Kamera kann nun, von jedem Computer der mit Ihrem Netzwerk verbunden ist angesteuert und über den Browser bedient werden.



ACHTUNG:
Unter Windows XP wird die Kamera nicht angezeigt bevor die benötigten Steuerelemente installiert wurden. Es erscheint lediglich die Meldung ***Diese Seite kann nicht angezeigt werden.*** ***Beachten Sie die Schritte im Abschnitt „Zugriff unter Windows XP“ (Seite 38) und befolgen Sie diese, um die Kamera anzeigen zu lassen und zu überprüfen, ob Sie über diese IP-Adresse erreicht werden kann.***

14. Beachten Sie die Hinweise im folgenden Abschnitt um auf die Kamera zuzugreifen. Danach können Sie die WLAN-Einstellungen (Seite 48) vornehmen und die grundlegenden Funktionen testen.

ZUGRIFF AUF DIE KAMERA

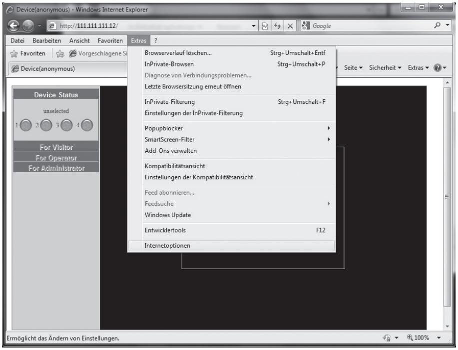
Das volle Menü der Kamera kann nur im Microsoft Internet Explorer angezeigt werden. Verwenden Sie daher keinen anderen Browser ◪, um auf die Kamera zuzugreifen.

Unter Windows 7 (und Vista)

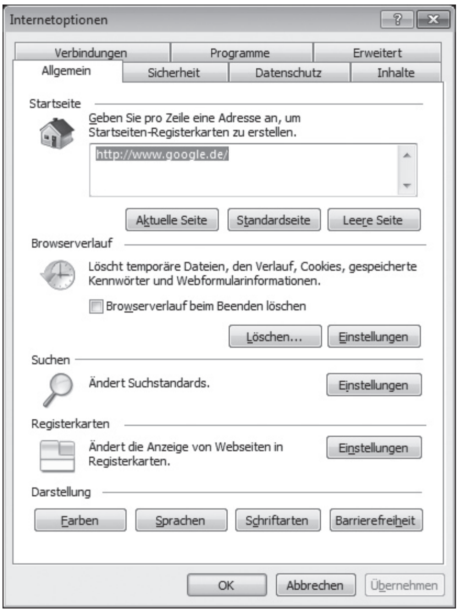
- **Sicherheitseinstellungen deaktivieren**

HINWEIS:
Für die Verwendung der Kamera müssen ActiveX-Steuerelemente auf Ihrem Computer installiert werden. Dies kann nur durchgeführt werden, wenn für die Dauer der Installation die Sicherheits-einstellungen des Internet Explorers deaktiviert werden. Die Sicherheitseinstellungen werden nach der Installation wiederhergestellt, damit Ihr System nicht gefährdet wird.

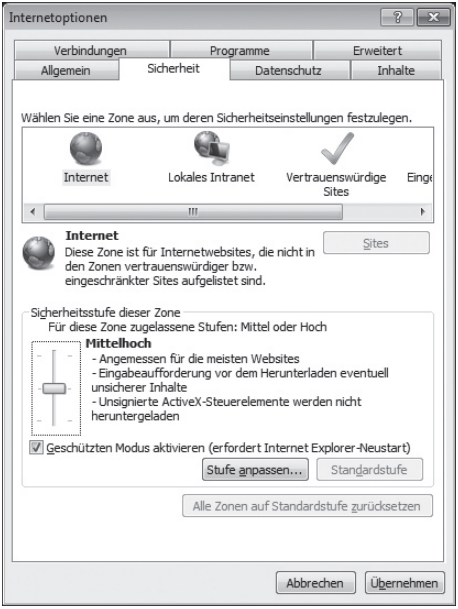
1. Öffnen Sie das Menü **Extras** Ihres Internet Explorers und wählen Sie den Reiter **Internetoptionen**.



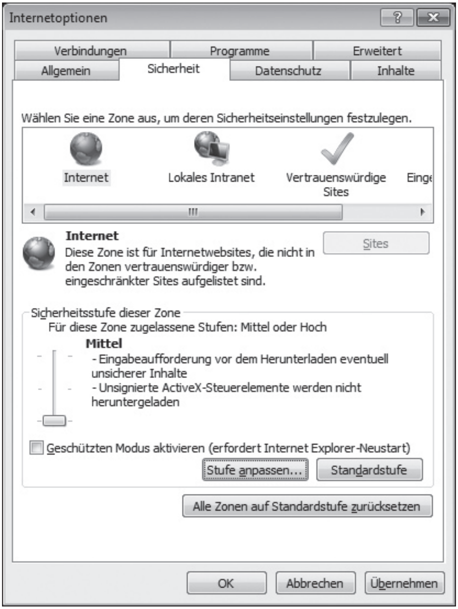
2. Es erscheinen die allgemeinen Internetoptionen. Klicken Sie auf **Sicherheit**.



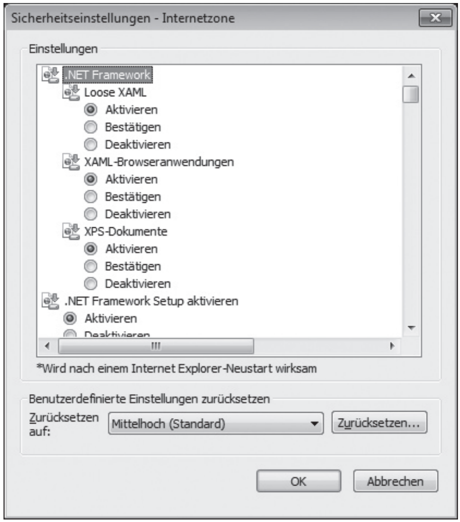
3. Fahren Sie mit der Maus in den Bereich **Sicherheitsstufe dieser Zone**. Die Sicherheitseinstellungen sind normalerweise auf **Mittelhoch** oder **Hoch**.



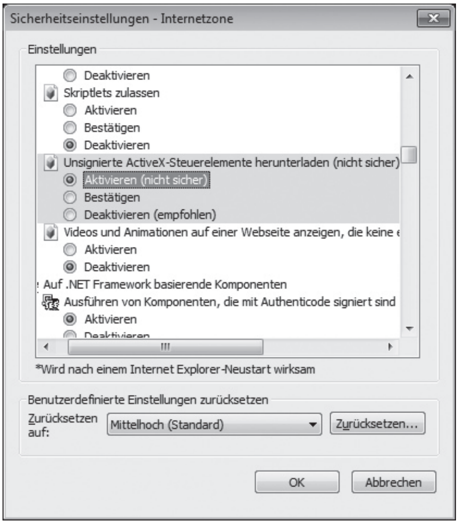
4. Ziehen Sie den Regler mit der Maus ganz nach unten auf **Mittel** und entfernen Sie den Haken bei **Geschützten Modus aktivieren**.



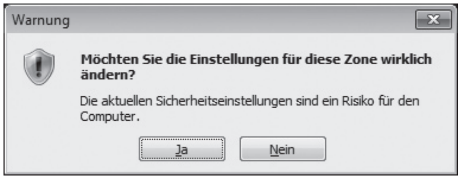
5. Klicken Sie auf **Stufe anpassen…**, um das Fenster **Sicherheitseinstellungen – Internetzone** zu öffnen.



6. Scrollen Sie nach unten, bis Sie den Punkt **Unsignierte ActiveX-Steuerlemente herunterladen** finden. Wählen Sie **Aktivieren (nicht sicher)** und klicken Sie auf **OK**.



7. Windows verlangt eine Bestätigung, um die Sicherheitseinstellungen zu ändern.
   Klicken Sie auf **Ja,** um fortzufahren.

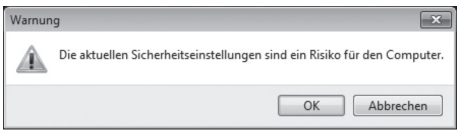


HINWEIS:
Windows zeigt Ihnen nun eine Meldung über die geänderten Einstellungen. In der Taskleiste erscheint ein neues Symbol über das Sie die Einstellungen später wieder bequem zurücksetzen können. Weitere Informationen hierzu erhalten Sie im Abschnitt ***Sicherheitseinstellungen wiederherstellen*** *(Seite 46).*

8. Klicken Sie auf **Übernehmen.**



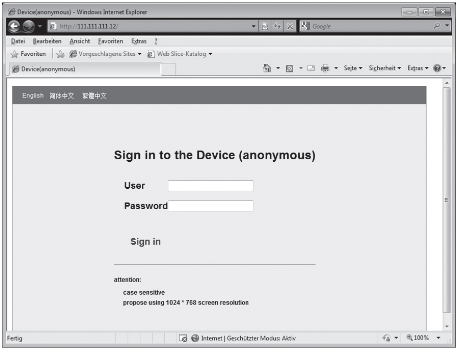
9. Diese Sicherheitseinstellungen werden von Windows nicht empfohlen und es erscheint eine entsprechende Warnmeldung. Klicken Sie **OK**, um fortzufahren.



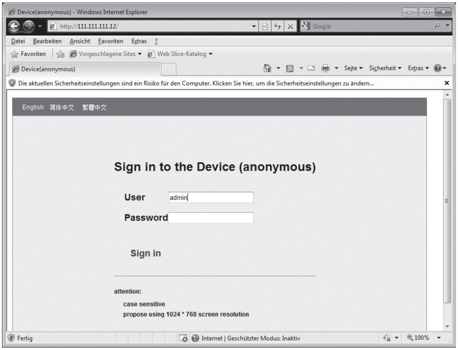
10. Die benötigten Steuerelemente können jetzt installiert werden und Sie können auf die Kamera zugreifen.

- **Zugriff auf die Kamera (Windows Vista/7)**

Geben Sie die IP-Adresse der Kamera in die Adresszeile des Internetexplorers ein. Warten Sie bis der Login-Schirm der Kamera geladen wurde.



Geben Sie dann Ihren USER-Namen und das Passwort ein. Werkseitig ist der USER-Name auf **admin** eingestellt und kein Passwort festgelegt. Verwenden Sie daher beim ersten Zugriff diese Daten und klicken Sie auf **Sign In.**



HINWEIS:
Nach dem einloggen versucht die Kamera ein ActiveX-Steuerelement zu installieren. In diesem Fall kann oben im Browser die folgende Warnmeldung erscheinen:
„Möchten Sie zulassen, dass durch das folgende Programm von einem unbekannten Herausgeber Änderungen an diesem Computer vorgenommen werden?“
Klicken Sie auf die Meldung und erlauben Sie die Installation. Der Login-Schirm wird neu geladen. Geben Sie den USER-Namen und das Passwort (siehe oben) erneut ein, um auf die Kamera zuzugreifen.

Sie können jetzt die grundlegende Verwendung ausprobieren und die WLAN-Einstellungen vornehmen. Beachten Sie hierzu auch die folgenden Abschnitte.

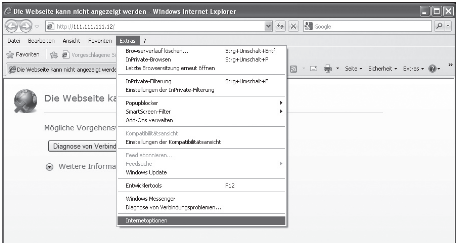
Unter Windows XP

ACHTUNG:
Für die Installation benötigen Sie eine aktuelle Version des Microsoft Internet Explorers. Vergewissern Sie sich, dass Sie alle aktuellen Updates installiert haben. Weitere Informationen erhalten Sie auf www.microsoft.com.

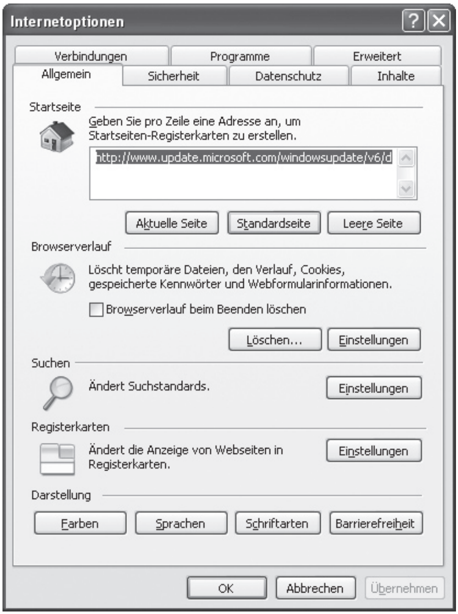
- **Sicherheitseinstellungen deaktivieren**
  Vor dem Abschluss der Installation wird der Login-Schirm der Kamera nicht angezeigt. Auch wenn Sie die richtige Adresse eingegeben haben zeigt der Browser nur die Meldung **Diese Seite kann nicht angezeigt werden**.

HINWEIS:
Für die Verwendung der Kamera müssen ActiveX-Steuerelemente auf Ihrem Computer installiert werden. Diese kann nur durchgeführt werden, wenn für die Dauer der Installation die Sicherheits-einstellungen des Internet Explorers deaktiviert werden. Die Sicherheitseinstellungen werden nach der Installation wiederhergestellt, damit Ihr System nicht gefährdet wird.

1. Öffnen Sie das Menü **Extras** Ihres Internet Explorers und wählen Sie den Reiter **Internetoptionen.**



2. Es erscheinen die allgemeinen Internetoptionen. Klicken Sie auf **Sicherheit**.



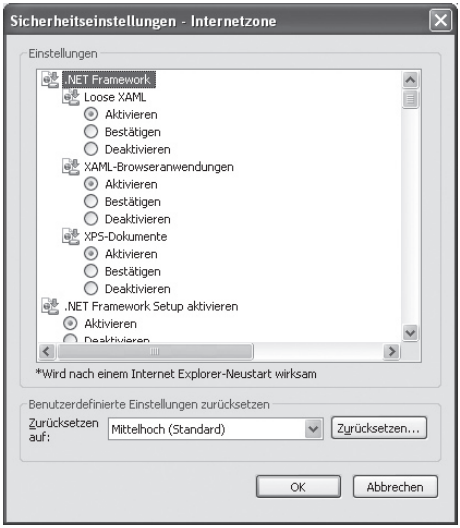
3. Fahren Sie mit der Maus in den Bereich **Sicherheitsstufe dieser Zone**. Die Sicherheitseinstellungen sind normalerweise auf **Mittelhoch** oder **Hoch**.



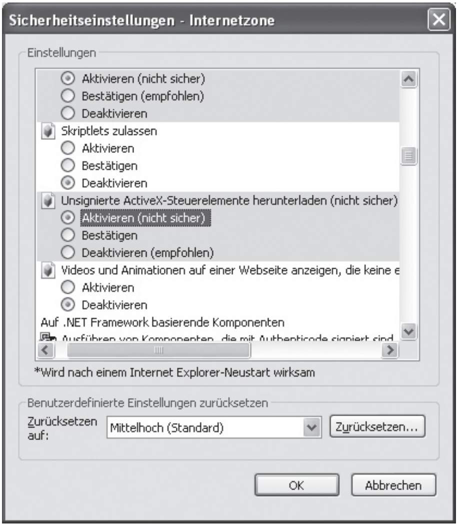
4. Ziehen Sie den Regler mit der Maus ganz nach unten auf **Mittel**.



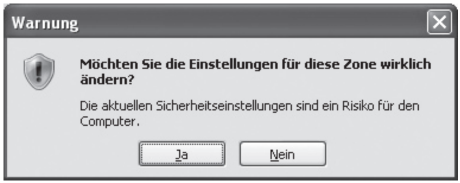
5. Klicken Sie auf **Stufe anpassen…**, um das Fenster **Sicherheitseinstellungen – Internetzone** zu öffnen.



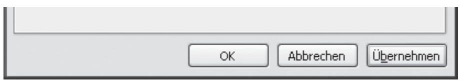
6. Scrollen Sie nach unten, bis Sie die Auswahlmenüs für ActiveX-Steuerelemente finden. Wählen Sie für jeden Punkt **Aktivieren (nicht sicher)** und klicken Sie auf **OK**.



7. Windows verlangt eine Bestätigung, um die Sicherheitseinstellungen zu ändern.
   Klicken Sie auf **Ja**, um fortzufahren.



8. Klicken Sie auf **Übernehmen**.

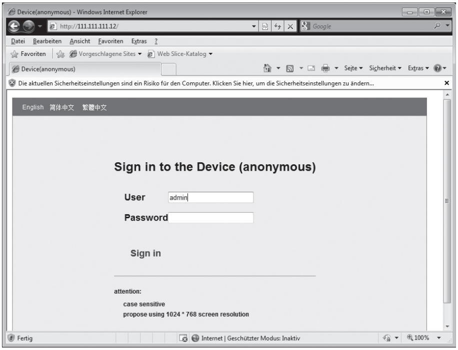


9. Die benötigten Steuerelemente können jetzt installiert werden und Sie können auf die Kamera zugreifen.

10. Geben Sie die IP-Adresse ➘ der Kamera in die Adresszeile des Internet Explorers ein. Die Login-Seite wird jetzt angezeigt.

- **Zugriff auf die Kamera (Windows XP)**
  Geben Sie die IP-Adresse der Kamera in die Adresszeile des Internet Explorers ein. Wenn Sie die Sicherheitseinstellungen wie im vorigen Abschnitt beschrieben deaktiviert haben, wird jetzt die Login-Seite der IP-Kamera geladen.

  Geben Sie dann Ihren USER-Namen und das Passwort ein. Werkseitig ist der USER-Name auf **admin** eingestellt und kein Passwort festgelegt. Verwenden Sie daher beim ersten Zugriff diese Daten und klicken Sie auf **Sign In**.

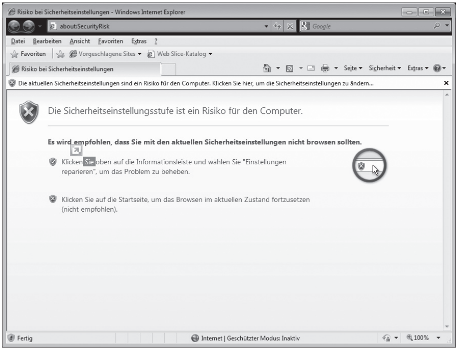


Sie können jetzt die grundlegende Verwendung ausprobieren und die WLAN-Einstellungen vornehmen. Beachten Sie hierzu auch die folgenden Abschnitte.

Sicherheitseinstellungen wiederherstellen

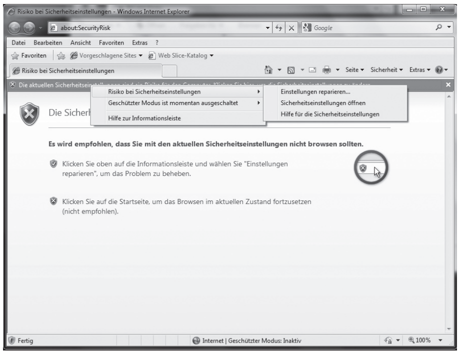
ACHTUNG:
Nach Abschluss der Installation sollten Sie unbedingt die Sicherheitseinstellungen des Microsoft Internet Explorers wiederherstellen, um Ihr System zu schützen.

Beim nächsten Start des Internet Explorers warnt Sie dieser, das die Sicherheitseinstellungen nicht ausreichend sind.

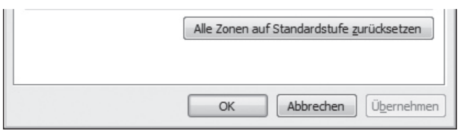


Folgen Sie den Anweisungen des Explorers hinter dem grünen Schild, um die Sicherheitseinstellungen wiederherzustellen.

1. Klicken Sie auf die Anzeige oben im Browserfenster und wählen Sie die Reiter **Risiko bei Sicherheitseinstellungen** und **Sicherheitseinstellungen öffnen**.



2. Wählen Sie im nächsten Fenster **Alle Zonen auf Standardstufe zurücksetzen**.



3. Klicken Sie auf **Übernehmen**, um den Vorgang abzuschließen.

Die Kamera kann jetzt verwendet werden. Fahren Sie mit dem Abschnitt „WLAN Einstellungen“ fort, wenn Sie die Kamera kabellos verwenden wollen. Gehen Sie direkt zum Abschnitt „Grundlegende Steuerung“ (Seite 56), wenn Sie die Kamera an einem Ethernetkabel betreiben wollen.

WLAN-EINSTELLUNGEN

Sie können die Kamera nun über das Netzwerkkabel betreiben oder mit Ihrem WLAN verbinden. Im folgenden Abschnitt wird die WLAN-Einstellung beschrieben. Wenn Sie die Kamera weiterhin per Kabel betreiben wollen, können Sie diesen Abschnitt überspringen und direkt mit „Montage" (Seite 55) fortfahren.

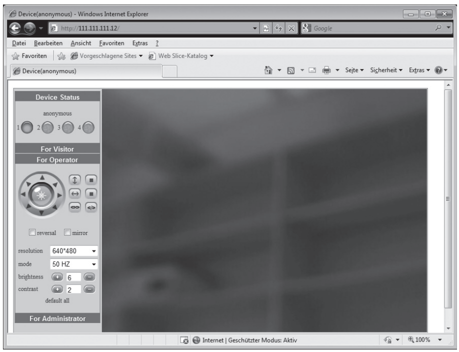
Damit die Kamera per WLAN betrieben werden kann, müssen zuerst die Zugangsdaten Ihres Netzwerkes eingegeben werden. Die Einstellungen können Sie nur vornehmen, während die Kamera noch per Kabel mit Ihrem Router verbunden ist. Folgen Sie den Schritten im vorherigen Abschnitt „Anschluss und Inbetriebnahme" und fahren Sie dann mit Punkt 1 dieses Abschnitts fort.

HINWEIS:
Versichern Sie sich, dass Ihr Router keine Whitelist ↘ verwendet, da die Kamera sich dann nicht mit dem Netzwerk verbinden kann. Sollte Ihr Netzwerk eine Whitelist verwenden, tragen Sie die IP-Adresse der Kamera in diese ein.

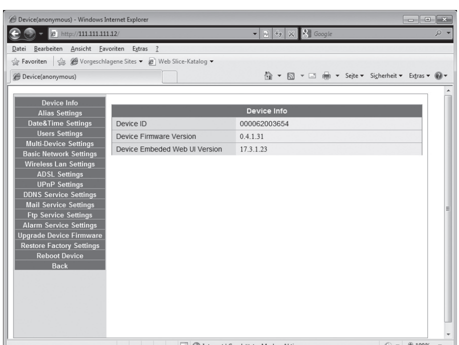
Verbindung einrichten

1. Loggen Sie sich wie in den vorherigen Abschnitten beschrieben auf der Startseite der IP-Kamera ein.

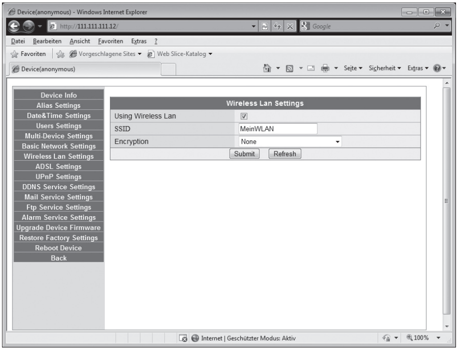
2. Klicken Sie auf **For Administrator.**



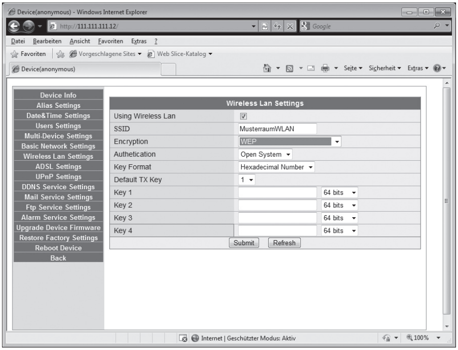
3. Die Seite für Administrator-Einstellungen wird nun geladen und die Grundinformationen des Gerätes angezeigt.



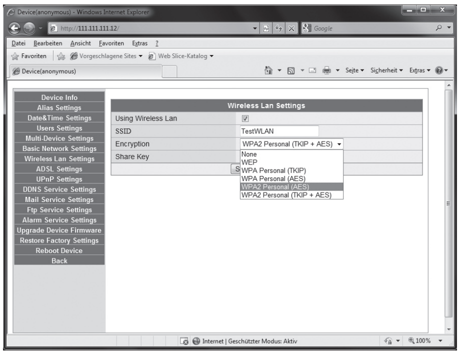
4. Klicken Sie auf **Wireless Lan Settings**.



5. Versichern Sie sich, dass der Haken bei **Using Wireless Lan** gesetzt ist.
6. Die Kamera versucht WLAN-Netzwerke automatisch zu erkennen. Überprüfen Sie, ob Ihr Netztwerk unter **SSID** angezeigt wird. Falls dies nicht der Fall ist, geben Sie Ihre Netzwerk SSID ◪ manuell ein.



7. Wählen Sie nun unter **Encryption** welche Verschlüsselung von Ihrem Netzwerk verwendet wird. Für genauere Informationen hierzu beachten Sie bitte die Hinweise im Handbuch Ihres WLAN-Routers. Falls Sie keine Verschlüsselung verwenden, klicken Sie auf **Submit** und fahren Sie mit Schritt 10 fort.

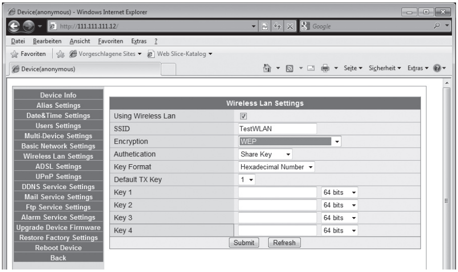


ACHTUNG:
Es wird unbedingt empfohlen Ihr Netzwerk durch eine WPA2-Verschlüsselung zu sichern. Genauere Informationen hierzu finden Sie im Anhang.

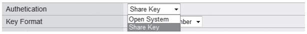
8. Falls Ihr Netzwerk eine WEP-Verschlüsselung verwendet befolgen Sie die Schritte im folgenden Abschnitt „WEP“ und fahren Sie dann mit „Verbinden“ (Seite 54) fort.
9. Falls Ihr Netzwerk eine WPA- oder WPA2-Verschlüsselung verwendet befolgen Sie die Schritte im folgenden Abschnitt „WPA und WPA2“ und fahren Sie dann mit „Verbinden“ (Seite 54) fort.
10. Klicken Sie auf **Submit,** um die Einstellungen zu speichern und fahren Sie mit dem Abschnitt „Verbinden“ (Seite 54) fort.

WEP

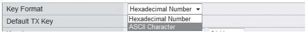
Mit den folgenden Schritten können Sie die IP-Kamera auf ein WEP geschütztes Netzwerk zugreifen lassen.



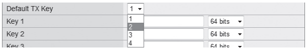
Wählen Sie zuerst **WEP** aus dem Dropdown-Menü, um die benötigten Eingabefelder zu öffnen.



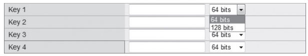
Wählen Sie aus, ob Sie ein offenes System oder einen Pre-Shared Key verwenden.



Stellen Sie hier ein, ob Ihre Netzwerkschlüssel im Hexadezimalsystem oder als ASCII-Zeichen eingegeben werden.



Wählen Sie hier den Schlüssel aus der von Ihrem Netzwerk als Standard verwendet wird.

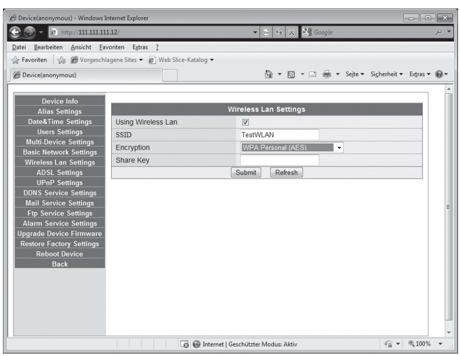


Geben Sie den Shared Key Ihres Netzwerks ein und geben Sie an, ob dieser eine 64 oder 128 Bit Verschlüsselung verwendet. Sie müssen nur den Key angeben, dessen Nummer Sie beim vorherigen Punkt angegeben haben.

Klicken Sie auf **Submit**, um die Einstellungen zu speichern und fahren Sie mit dem Abschnitt „Verbinden“ im nächsten Abschnitt fort. Die Kamera startet sich neu, um die neuen Einstellungen zu laden.

WPA und WPA2

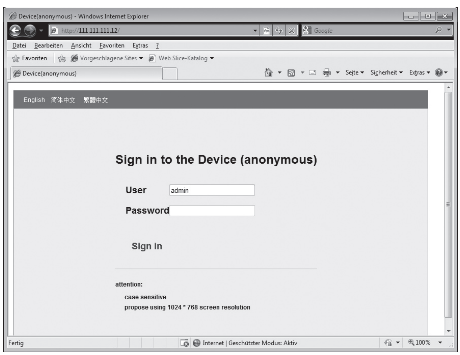
Mit den folgenden Schritten können Sie die IP-Kamera auf ein WPA oder WPA2 ➘ geschütztes Netzwerk zugreifen lassen.



Wählen Sie die verwendete WPA Sorte und geben Sie den Pre-Shared Key ➘ ein. Klicken Sie auf **Submit**, um die Einstellungen zu speichern und fahren Sie mit dem Abschnitt „Verbinden“ im nächsten Abschnitt fort.

Verbinden

Nach dem die Einstellungen der vorherigen Abschnitte vorgenehmen werden können Sie die IP-Kamera auch kabellos ansteuern. Trennen Sie das Ethernetkabel und schrauben Sie die Antenne hinten an die IP-Kamera. Starten Sie dann Ihren Internet Explorer neu und geben Sie die IP-Adresse der Kamera erneut ein. Die Login-Seite der Kamera wird geladen.



Geben Sie den Benutzernamen und das Passwort erneut ein. Der Zugriff auf die Kamera erfolgt auf die gleiche Weise wie in den Abschnitten „Zugriff auf die Kamera“ (Seite 28) beschrieben.

MONTAGE

Nachdem die IP-Kamera betriebsbereit gemacht wurde und in Ihrem Netzwerk erkannt wurde, kann diese montiert werden. Montieren Sie die Kamera an einem wettergeschützen Ort und versichern Sie sich, dass die Kamera den von Ihnen gewünschten Bereich überwachen kann und ob Sie sich im Empfangsbereich Ihres WLAN-Routers befindet. Die maximale Reichweite für eine Stabile WLAN-Verbindung beträgt durchschnittlich 30 Meter.

1. Verschrauben Sie die Halterung fest mit einer Wand.
2. Setzen Sie die Kamera auf die Halterung und drehen Sie die Schraube fest, bis die Kamera nicht mehr bewegt werden kann.
3. Drehen Sie die Winkeleinstellung der Halterung bis die Kamera in der gewünschten Position ist.

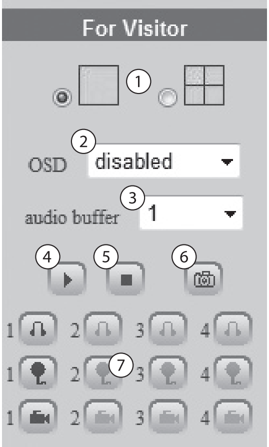


GRUNDLEGENDE STEUERUNG

Nach dem Einloggen werden Ihnen das Kamerabild und das Bedienfeld angezeigt. Als Administrator können Sie auf den vollen Funktionsumfang der Kamera zugreifen. Die Bedienelemente sind jedoch je nach Sicherheitsstufe, in den einzelnen Berechtigungsstufen einsortiert.



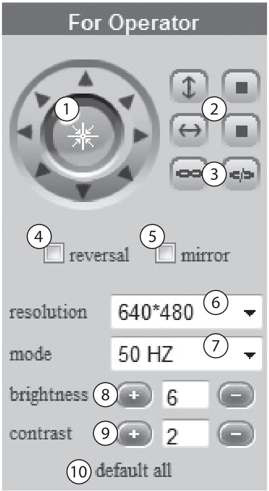
Über die Browsersteuerung können Sie bis zu 4 Kameras gleichzeitig steuern. Erkannte IP-Kameras werden grün angezeigt.



1. Auswahl zwischen einem einzelnen Bild oder vier Ausschnitten von allen Kameras anzeigen lassen.
2. Auswahl, ob und in welcher Farbe das On Screen Display angezeigt werden soll. Das Display blendet Zeit und Datum unten am rechten Bildrand ein.
3. Stufe des Audio-Buffers.
4. Starten der Kameraanzeige.
5. Beenden der Kameraanzeige.
6. Schnappschussauslöser.
7. Kamerazugriffsfelder. Die einzelnen Kameras können hier direkt angesteuert werden.

	Aktiviert die Tonaufnahme der Kamera und erlaubt Ihnen mitzuhören.
	Aktiviert das Mikrofon der Kamera und erlaubt Ihnen durch die Kamera zu sprechen, falls Sie ein entsprechendes Aufnahmegerät an Ihren Computer angeschlossen haben.
	Startet eine Videoaufnahme. Durch erneutes Klicken wird die Aufnahmen beendet und gespeichert.

HINWEIS:
Beim Start einer Aufnahme können Sie wählen wo und unter welchem Namen die Datei gespeichert werden soll. Die Aufnahmen werden als AVI-Dateien gespeichert.



1. Steuerfeld zum Bewegen der Kamera
2. Patrouillenfunktion
3. Ein-/Ausschalten
4. Bild drehen
5. Bild spiegeln
6. Auflösung
7. Modus
8. Helligkeit
9. Kontrast
10. Alle Werte in diesem Menü auf Werkseinstellungen setzen

Device Info	
Device ID	000062003654
Device Firmware Version	0.4.1.31
Device Embeded Web UI Version	17.3.1.23

Die Einstellungen für Operator sollten nur von erfahrenen Benutzern verwendet werden. Eine detaillierte Beschreibung der einzelnen Funktionen finden Sie in der ausführlichen Bedienungsanleitung auf www.pearl.de. Jeder Benutzer sollte allerdings gleich zu Beginn einen neuen Benutzernamen und ein Passwort festlegen, um die Kamera vor unbefugtem Zugriff zu schützen. Befolgen Sie dafür die folgenden Schritte.

1. Klicken sie auf **User Settings**.
2. Ändern Sie im obersten Feld das Wort **admin** zu dem Benutzernamen den Sie verwenden wollen.
3. Tragen Sie im Feld **Password** dahinter das Passwort ein, das Sie verwenden wollen.
4. Klicken Sie auf **Submit,** um die Einstellungen zu speichern.
5. Von jetzt an werden der von Ihnen festgelegte Benutzername und das neue Passwort benötigt, um über die Login-Seite der IP-Kamera auf diese zuzugreifen.

Users Settings

User	Password	Group
admin		Administrator
		Visitor
		Visitor
		Visitor
		Visitor
		Visitor
		Visitor
		Visitor

Submit Refresh

ANHANG

LÖSUNG HÄUFIGER PROBLEME (TROUBLESHOOTING)

Die Kamera wird im Netzwerk nicht erkannt

1. Überprüfen Sie, ob die IP-Adresse der Kamera im selben Subnetz liegt wie Ihr restliches Netzwerk.
2. Versichern Sie sich, dass die der Kamera zugewiesenen IP- Und Mac-Adresssen nicht schon an andere Geräte Ihres Netzwerks vergeben sind.
3. Überprüfen Sie Schritt für Schritt die Netzwerkeinstellungen der IP-Kamera.
4. Versichern Sie sich, dass Ihr Router eingehende Signale von Port 80 erlaubt.
5. Überprüfen Sie, ob Ihr Router Port Forwarding aktiviert hat.

Das Passwort und/oder der Benutzername sind verloren gegangen.

Die einzige Möglichkeit wieder auf die Kamera zuzugreifen ist die Werkseinstellungen wiederherzustellen. An der Unterseite der Kamera befindet sich eine versenkte Reset-Taste. Verwenden Sie eine Büroklammer oder einen ähnlichen Gegenstand, um diese Taste für mehrere Sekunden zu drücken. Die Kamera wird zurückgesetzt und kann wieder mit dem Benutzernamen **admin** und ohne Passwort verwendet werden.

ACHTUNG:

Durch das Wiederherstellen der Werkseinstellungen werden alle vorgenommen Einstellungen gelöscht. Alle Benutzerdaten gehen verloren, die Zugangsdaten zu Ihrem Netzwerk sind gelöscht und die IP-Kamera muss vollständig neu eingerichtet werden. Führen Sie diesen Vorgang daher nicht leichtfertig aus.

Die Bilderübertragungsrate ruckelt und/oder ist von schlechter Qualität.
Die Übertragung wird von mehreren Faktoren wie der genutzten Bandbreite, der Anzahl der IP-Kameras, der Prozessorleistung Ihres Computers, der Anzahl der Zugriffe, Störsignale im WLAN (auf der 2,4 GHz Frequenz) und den Modus- und Helligkeitseinstellungen beeinflusst. Überprüfen Sie, ob einer dieser Faktoren ungewöhnlich hoch oder niedrig ist, um das Problem zu identifizieren. Fall Ihr Netzwerk noch Hubs verwendet tauschen Sie diese durch Netzwerk-Switches aus, um eine bessere Übertragung zu sichern.

BASISWISSEN NETZWERKE

Da bei Netzwerken häufig Unklarheiten und missverständliche Begriffe auftreten, soll dieses Glossar dabei helfen, Licht ins Dunkel mancher Fachbegriffe zu bringen. Im Folgenden werden die grundlegenden Hardwarekomponenten eines herkömmlichen Heimnetzwerks ebenso dargestellt, als auch die verwendeten Anwendungen und Dienste.

Hardware

- **Access-Point**
  Der Zugangspunkt oder auch Access-Point ist die „Basisstation" in einem drahtlosen Netzwerk (WLAN). Diese Funktion wird häufig in Heimnetzwerken auch von einem Router ↘ übernommen.

- **DSL-Modem**
  Das DSL-Modem verbindet Ihren Computer mit dem Internet. Wenn Sie mit mehr als einen Computer über eine Leitung Zugriff auf das Internet haben wollen, benötigen Sie einen Router ↘, der direkt hinter das DSL-Modem geschalten wird.

- **Kabelmodem**
  Als Kabelmodem bezeichnet man das Gerät, das Daten Über Fernseh-Kabelnetze überträgt und für Breitband-Internetzugänge über Kabelanschlüsse (Kabelinternet) eingesetzt wird.

- **Netzwerkkabel/Ethernetkabel**
  Hier gibt es zwei Varianten. So genannte „Patch"-Kabel und „Crossover"-Kabel. Patchkabel sind die Kabel, die am häufigsten Verwendung in Netzwerken finden. Sie werden eingesetzt um Computer mit Switches ↘, Hubs ↘ oder Routern ↘ zu verbinden.

Crossover-Kabel werden dazu eingesetzt um zwei Computer direkt miteinander zu verbinden, ohne ein Netzwerk zu verwenden. Patchkabel sind der gängige Lieferumfang von Netzwerkprodukten.

- **Netzwerkswitch**
  Switches werden als „Knotenpunkt“ von Netzwerken eingesetzt. Sie dienen dazu mehrere Netzwerkgeräte „auf ein Kabel“ im Netzwerk zusammenzuführen. Switches sind häufig zu logischen Verbünden zusammengestellt und verbinden z.B. alle Computer aus einem Büro. Koppelt man mehrere Switches erhält man ein komplexeres Netzwerk, welches einer Baumstruktur ähnelt.

- **Router**
  Router dienen zur Zugriffssteuerung von Netzwerkcomputern untereinander und regeln ebenfalls den Zugriff auf das Internet für alle sich im Netzwerk befindlichen Computer. Router werden sowohl rein kabelgebunden, als auch als WLAN-fähige Variante vertrieben. Meist übernehmen handelsübliche Router noch Sonderfunktionen wie z.B. DHCP ↘, QoS ↘, Firewall ↘, NTP ↘,…

Grundlegende Netzwerkbegriffe

- **Adressbereich**
  Ein Adressbereich ist eine festgelegte Gruppe von IP- oder MAC-Adressen ↘ und fast diese zu einer „Verwaltungseinheit“ zusammen.

- **Blacklist**
  Mit einer Blacklist bezeichnet man bei Netzwerken eine Liste von Geräten denen die Verbindung zu einem Gerät (z.B. Router) explizit nicht erlaubt ist. Alle anderen Geräte werden von dem Gerät akzeptiert, das den Zugang über die Blacklist regelt. Im Gegensatz dazu steht die so genannte Whitelist ↘.

- **Browser**
  Browser werden Programme genannt die hauptsächlich zur Darstellung von Webseiten genutzt werden. Die bekanntesten Browser sind mitunter der Internet Explorer, Mozilla Firefox, Opera oder Google Chrome.

- **Client**
  Als Client wird jede Anwendung bezeichnet, die Daten eines Serverdienstes in Anspruch nimmt. Eine klassische Client-Server Bindung entsteht in Heimnetzwerken häufig schon bei der Vergabe von IP-Adressen im Netzwerk. Hier fordert der Computer als DHCP-Client ↘ eine gültige IP-Adresse vom DHCP-Server (meist der Router) an und erhält diese vom DHCP-Server zugeteilt.

- **IP-Adresse**
  IP-Adressen werden dazu verwendet Computer, Drucker oder andere Geräte flexibel in ein Netzwerk einzubinden. Hierbei ist zwischen globalen und privaten IP-Adressen zu unterscheiden. Globale IP-Adressen werden von den einzelnen Internet-Anbietern oftmals dynamisch (DHCP ↘) vergeben. Sie dienen dazu, Ihr Heimnetzwerk oder auch nur den einzelnen Computer gegenüber dem Internet erreichbar zu machen.

Private IP-Adressen werden im Heimnetzwerk entweder statisch („von Hand" zugewiesen) oder dynamisch (DHCP) vom Anwender selbst vergeben. IP-Adressen ordnen ein spezielles Gerät eindeutig einem bestimmten Netzwerk zu.

Beispiel:
IP-Adressen sind die bekanntesten Adressierungen im Netzwerk und treten in folgender Form auf: z.B. 192.168.0.1

- **ISP**
  ISP ist die Abkürzung für „Internet Service Provider".
  Dieser Begriff wird für Stellen verwendet, die einem Netzwerk oder Einzelcomputer den Zugang zum Internet anbieten. In Deutschland ist der wohl bekannteste ISP T-Online, aber auch Anbieter wie Freenet, Arcor, 1&1 oder KabelDeutschland gehören zu den ISPs.

- **LAN**
  LAN (Local Area Network) bezeichnet ein Netzwerk aus Computern und anderen Netzwerkgeräten, die über einen gemeinsamen Adressbereich ↘ verfügen und damit zu einer Struktur zusammengefasst werden.

- **Passphrase**
  Mit dem Begriff Passphrase wird ein Schlüsselwort oder Satz umschrieben, der als Sicherheitsabfrage bei der Verbindung zu WPA-/WPA2-Verschlüsselten ↘ Netzwerken eingegeben werden muss.

- **Port**
  Als Port wird eine Softwareschnittstelle bezeichnet, die es einzelnen Anwendungen auf Ihrem Computer ermöglicht mit den Anwendungen eines Anbieters zu kommunizieren. Hier wird hauptsächlich zwischen zwei Protokollen unterschieden: TCP ↘ und UDP ↘.

  Beispiel:
  Die häufigste Internet Anwendung ist ein Browser ↘ (Internet Explorer, Mozilla Firefox, usw.), welcher meist über den TCP-Port 80 mit den Servern ↘ der Webseiten-Anbieter kommuniziert.

- **Protokoll**
  Protokolle im Netzwerk sind Standards für Datenpakete, die Netzwerkgeräte untereinander austauschen, um eine eindeutige Kommunikation zu ermöglichen.

- **Pre-Shared Key**
  Mit Pre-Shared Key („vorher vereinbarter Schlüssel“) oder kurz PSK bezeichnet man ein Verschlüsselungsverfahren ↘, bei denen die verwendeten Schlüssel vor der Verbindung beiden Teilnehmern bekannt sein muss (siehe auch WPA/WPA2 ↘.

- **MAC-Adresse**
  Als MAC-Adresse bezeichnet man die physikalische Adresse einer Netzwerkkomponente (z.B. Netzwerkkarte ↘, WLAN-Dongle ↘, Drucker, Switch ↘). MAC-Adressen sind entgegen IP-Adressen ↘ immer eindeutig zuordenbar. MAC-Adressen von anderen verbundenen Netzwerkgeräten werden von den einzelnen Geräten jeweils in einer so genannten ARP-Tabelle gespeichert. Diese ARP-Tabellen können zur Fehlersuche dienen, falls ein Gerät ohne IP-Adresse (z.B. Switch) im Netzwerk keine Funktion zeigt.

  Beispiel:
  Eine MAC-Adresse sieht z.B. so aus: 00:00:C0:5A:42:C1

- **Sichere Passwörter**
  Unter sicheren Passwörtern versteht man Passwörter, die bestimmte Bedingungen erfüllen, um von Angreifern nicht mit einfachsten Mitteln entschlüsselt werden zu können. Sichere Passwörter sollten generell eine bestimmte Mindestlänge aufweisen und mehrere Sonderzeichen beinhalten. Als Faustregel gilt hier: Je länger das Passwort ist und je mehr Sonderzeichen es beinhaltet, desto sicherer ist es gegen Entschlüsselung.

- **SSID**
  SSID (Service Set Identifier) steht für die Bezeichnung, die für ein WLAN-Netzwerk verwendet wird. Diese SSID wird meist per Broadcast (siehe UDP ◪) öffentlich ausgesendet, um das Netzwerk für mobile Geräte „sichtbar" zu machen.

- **Subnetz**
  Subnetze sind eine Zusammenfassung von einzelnen IP-Adressen ◪ zu Netzwerkstrukturen. So werden meist Computer einer Abteilung im Büro in einem Subnetz zusammengefasst, während die Computer einer anderen Abteilung in einem weiteren Subnetz zusammengefasst sind. Daher sind Subnetze eine reine Strukturierungsmaßnahme. Eine Angabe des Subnetzraumes wird immer in Zusammenhang mit der Vergabe einer IP-Adresse durchgeführt. Im Heimbereich werden normalerweise keine speziellen Subnetze eingerichtet. Daher ist bei Windows-Systemen als Subnetzmaske die 255.255.255.0 voreingestellt. Dadurch stehen die IP-Adressen xxx.xxx.xxx.1 bis xxx.xxx.xxx.254 zur Verfügung.

- **TCP (Transmission Control Protocol)**
  Das TCP-Protokoll wird dazu verwendet gezielt Informationen von einem speziellen Gegenüber abzufragen (siehe Beispiel bei Port ◪)

- **UDP (User Datagram Protocol)**
  Das UDP-Protokoll ist ein so genanntes „Broadcast"-Protokoll. Broadcast wird im englischen auch für Radio- oder TV-Sendungen verwendet. Ganz ähnlich arbeitet dieses Protokoll ➘. Es wird verwendet, um Datenpakete an alle im Netzwerk erreichbaren Geräte zu senden und im Weiteren auf Rückmeldung dieser Geräte zu warten. Das UDP-Protokoll wird meist dann von Anwendungen eingesetzt, wenn unsicher ist ob eine entsprechende Gegenstelle im Netzwerk vorhanden ist.

- **uPNP**
  Mit diesem Begriff wird das „universal Plug and Play"-Protokoll bezeichnet. Dieses Protokoll ➘ wird hauptsächlich dazu verwendet, Drucker und ähnliche Peripheriegeräte über ein Netzwerk ansteuern zu können.

- **Verschlüsselung**
  Verschlüsselungsmechanismen werden in Netzwerken dazu eingesetzt, Ihre Daten vor fremdem Zugriff abzusichern. Diese Verschlüsselungsmechanismen funktionieren ähnlich wie bei einer EC-Karte. Nur mit dem richtigen Passwort (der richtigen PIN) können die Daten entschlüsselt werden.

- **VPN**
  VPN (Virtual Private Network) steht für eine Schnittstelle in einem Netzwerk, die es ermöglicht, Geräte an ein benachbartes Netz zu binden, ohne dass die Netzwerke zueinander kompatibel sein müssen.

- **WAN**
  WAN (Wide Area Network) bezeichnet ein Netzwerk aus Computern und anderen Netzwerkgeräten, die über größere Entfernungen und aus vielen Bestandteilen zusammengefasst werden. Das bekannteste Beispiel ist das „Internet". Jedoch kann ein WAN auch nur aus zwei räumlich voneinander getrennten LANs ➘ bestehen.

- **Whitelist**
  Mit einer Whitelist bezeichnet man bei Netzwerken eine Liste von Geräten denen die Verbindung zu einem Gerät (z.B. Router) explizit erlaubt ist. Alle anderen Geräte werden von dem Gerät abgewiesen, das den Zugang über die Whitelist regelt. Im Gegensatz dazu steht die so genannte Blacklist ➘.

Dienste in Netzwerken

- **DHCP (Dynamic Host Configuration Protocol)**
  Mit DHCP wird die dynamische Verteilung von IP- Adressen ↘ in Netzwerken bezeichnet. Dynamisch sind diese Adressen deshalb, weil Sie jederzeit ohne größeren Aufwand neu vergeben werden können. Man kann dynamische IP-Adressen auch als geliehene IP-Adressen bezeichnen. Diese geliehenen IP-Adressen werden mit einem „Verfallsdatum“ versehen – der so genannten „Lease Time“. Ein Computer wird am DHCP-Server nur dann nach einer neuen IP-Adresse anfragen, wenn sein „Lease“ abgelaufen ist. Dies ist allerdings auch eine mögliche Fehlerquelle, da es hier zu Unstimmigkeiten zwischen DHCP-Server und DHCP-Clients kommen kann.

  HINWEIS:
  Windows Computer sind standardmäßig als DHCP-Client eingestellt, um einen einfachen Anschluss an ein Heimnetzwerk zu ermöglichen.

- **DNS (Domain Name Server)**
  DNS ist ein Serverdienst, der die Übersetzung von IP-Adressen ↘ in gängige Internet-Adressen übernimmt. So wird z.B. aus www.google.de die IP-Adresse: 74.125.39.105. Werden Sie während einer Konfiguration aufgefordert, die DNS-IP-Adresse einzugeben, ist damit immer die Adresse desjenigen Servers ↘ gesucht, welcher den DNS-Serverdienst anbietet. DNS-Server werden aus Gründen der Ausfallsicherheit meist doppelt angegeben und als Primärer DNS (oder DNS1), bzw. Sekundärer DNS (oder DNS2) bezeichnet.

- **Filter**
  Siehe auch Firewall ↘

- **Firewall**
  Eine Firewall ist ein Sicherungsmechanismus, welcher meist auf Routern ◪ als Serverdienst läuft, jedoch bereits in Windows (seit XP) integriert ist. Sie erlaubt nur Zugriffe auf voreingestellte Ports ◪, blockt vorher konfigurierte IP-Adressen ◪ und soll generell schädliche Angriffe auf Ihr Netzwerk verhindern.

- **FTP/NAS (File Transfer Protocol/ Network Access Storage)**
  FTP ist ein Serverdienst, der hauptsächlich zum Transfer von Dateien verwendet wird. Dieser Dienst ermöglicht es auf unkomplizierte Art und Weise Dateien von einem Computer auf einen entfernt stehenden anderen Computer ähnlich dem Windows Explorer zu übertragen. So genannte NAS-Server setzen ebenfalls häufig diesen Dienst ein, um einen Zugriff aus dem gesamten Netzwerk auf eine Festplatte zu erlauben.

- **(Standard-) Gateway**
  Als Gateway wird die Schnittstelle bezeichnet, die es den Computern im privaten Netzwerk ermöglicht mit Computern außerhalb zu kommunizieren. Es ist in diesem Sinne mit Ihrem Router ◪ gleichzusetzen. Das Gateway sammelt und sendet Anfragen der Clients ◪ und leitet diese weiter an die entsprechenden Server ◪ im Internet. Ebenso verteilt das Gateway die Antworten der Server wieder an die Clients, die die Anfrage gestellt hatten.

- **HTTP/Webserver (Hypertext Transfer Protocol)**
  Dieser Dienst ist das, was in der Öffentlichkeit als „Das Internet" bezeichnet wird. Jedoch handelt es sich hier bei nur um eine Vereinfachung, da das Internet an sich eine übergeordnete Struktur ist, welche nahezu alle Serverdienste beinhaltet. HTTP wird zum Transfer und der Darstellung von Webseiten verwendet.

- **Mediastreams**
  Diese Gruppe von Serverdiensten wird von vielfältigen Geräten und Anbietern verwendet. Die bekanntesten Beispiele sind Internet-Radiosender, Video-On-Demand und IP-Kameras. Diese Streams nutzen teils unterschiedliche Protokolle ➘ und Protokollversionen. Daher kann es hier durchaus einmal zu Inkompatibilitäten zwischen Server ➘ und Client ➘ kommen.

- **NTP**
  NTP (Network Time Protcol) bezeichnet ein Protokoll ➘, mit dem Computer über das Netzwerk Ihre Datums- und Zeiteinstellungen abgleichen können. Dieser Dienst wird von weltweit verteilten Servern bereitgestellt.

- **PPPoE**
  PPPoE steht für PPP over Ethernet und bezeichnet Verwendung des Netzwerkprotokolls Point-to-Point Protocol (PPP) über eine Ethernet-Verbindung. PPPoE wird in Deutschland hauptsächlich in Verbindung mit ADSL-Anschlüssen verwendet. ADSL bedeutet Asynchrones DSL und steht für die Verwendung einer Leitung für Telefon und Internet. ADSL ist Standard in Deutschland. Hauptgrund für die Verwendung von PPPoE ist die Möglichkeit, Authentifizierung und Netzwerkkonfiguration (IP-Adresse ➘, Gateway ➘) auf dem schnelleren Ethernet zur Verfügung zu stellen.

- **Samba/SMB**
  Mit diesen Begriffen ist ein Serverdienst gemeint, der speziell in Windows Netzwerken verwendet wird. Dieser Service ermöglicht ebenfalls den schnellen und einfachen Zugriff auf Dateien die sich auf anderen Computern befinden (in so genannten „freigegebenen Ordnern"). Jedoch ist dieser Dienst auf Heimnetzwerke begrenzt und kann nur in Ausnahmefällen auch über das Internet in Anspruch genommen werden.

- **Server/Serverdienst**
  Ein Server ist immer als Anbieter von Netzwerkdiensten zu sehen. Einzelne Anwendungen werden auch als Serverdienst bezeichnet. Die bekanntesten Serverdienste sind unter anderem Webserver, DHCP oder E-Mail Server. Mehrere solche Dienste können auf einem Computer oder anderen Geräten (z.B. Routern) gleichzeitig verfügbar sein. Server werden auch Computer genannt, deren ausschließliche Funktion darin besteht Serverdienste anzubieten und zu verwalten.

- **Statische Adressvergabe**
  Bei der statischen Adressvergabe sind alle Netzwerkadressen eines Netzwerkes fest vergeben. Jeder einzelne Client (Computer) des Netzwerks hat seine feste IP-Adresse, die Subnetzmaske, das Standard-Gateway und den DNS-Server fest eingespeichert und muss sich mit diesen Daten beim Server anmelden.
  Ein neuer Client (Computer) muss erst mit einer gültigen, noch nicht vergebenen IP-Adresse und den restlichen Daten ausgestattet werden, bevor er das Netzwerk nutzen kann. Manuelle Adressvergabe ist besonders bei Netzwerkdruckern oder ähnlichen Geräten sinnvoll, auf die häufig zugegriffen werden muss oder in Netzwerken, die besonders sicher sein müssen.

- **WEP und WPA**
  Wired Equivalent Privacy (WEP) ist der ehemalige Standard-Verschlüsselungsalgorithmus für WLAN. Er soll sowohl den Zugang zum Netz regeln, als auch die Vertraulichkeit der Daten sicherstellen. Aufgrund verschiedener Schwachstellen wird das Verfahren als unsicher angesehen. Daher sollten WLAN-Installationen die sicherere WPA-Verschlüsselung verwenden. Wi-Fi Protected Access (WPA) ist eine modernere Verschlüsselungsmethode für ein WLAN. Sie wurde als Nachfolger von WEP eingeführt und weist nicht deren Schwachstellen auf.

SICHERHEITSMASSNAHMEN IN WLAN-NETZWERKEN

An erster Stelle sollten der Verzicht von WEP und der Einsatz von WPA oder WPA2 stehen. Dieses Ziel lässt sich in vielen Fällen bereits durch ein Treiber- oder Firmwareupdate erreichen. Lässt sich der Einsatz von WEP nicht vermeiden, sollten folgende grundlegende Behelfsmaßnahmen beachtet werden, um das Risiko von Angriffen fremder Personen auf das WLAN zu minimieren:

- Aktivieren Sie auf alle Fälle den Passwortschutz! Ändern Sie ggf. das Standard-Passwort des Access Points.
- Wenn Sie die WEP-Verschlüsselung verwenden, weil eines der angeschlossenen Geräte WPA oder WPA2 (dringend empfohlen) nicht unterstützt wird, sollte der WEP-Schlüssel mindestens 128 Bit lang sein und eine lose Kombination aus Buchstaben, Ziffern und Sonderzeichen darstellen.
- Aktivieren Sie die Zugriffskontrollliste (ACL = Access Control List), um vom Access Point nur Endgeräte mit bekannter MAC-Adresse zuzulassen. Beachten Sie, dass sich eine MAC-Adresse aber mittels Treiber beliebig einstellen lässt, sodass eine mitgelesene zugelassene MAC-Adresse leicht als eigene ausgegeben werden kann.
- Verwenden Sie eine sinnvolle SSID: Die SSID des Access Point sollte keine Rückschlüsse auf Ihren Namen, verwendete Hardware, Einsatzzweck und Einsatzort zulassen.
- Umstritten ist die Deaktivierung der SSID-Übermittlung (Broadcasting). Sie verhindert das unabsichtliche Einbuchen in das WLAN, jedoch kann die SSID bei deaktiviertem Broadcasting mit einem so genannten Sniffer (Gerät zur LAN-Analyse) mitgelesen werden, wenn sich etwa ein Endgerät beim Access Point anmeldet.
- WLAN-Geräte (wie der Access Point) sollten nicht per WLAN konfiguriert werden, sondern ausschließlich über eine kabelgebundene Verbindung.

- Schalten Sie WLAN-Geräte stets aus, wenn Sie sie nicht benutzen.
- Führen Sie regelmäßige Firmware-Updates vom Access Point durch, um sicherheitsrelevante Aktualisierungen zu erhalten.
- Reichweite des WLANs durch Reduzierung der Sendeleistung bzw. Standortwahl des WLAN Gerätes beeinflussen (Dies dient allerdings nicht der aktiven Sicherheit, sondern begrenzt lediglich den möglichen Angriffsbereich.)

Alle diese Sicherheitsmaßnahmen dürfen aber nicht darüber hinwegtäuschen, dass diese letztlich keinen wirklichen Schutz beim Einsatz von WEP bedeuten. Ein erfolgreicher Angriff auf die WEP-Verschlüsselung ist trotz all dieser Vorkehrungen mit den richtigen technischen Voraussetzungen innerhalb von 5 bis 10 Minuten mit ziemlicher Sicherheit erfolgreich.

CHECKLISTE FÜR DIE KONFIGURATION

Aufgabe	Erledigt
Funkkameraüberwachung ausschalten	
Schnurlostelefon ausschalten	
Sonstige Geräte mit 2,4 GHz ausschalten	
Stromversorgung mit Überspannungsschutz sichern	
Firewall am Computer ausstellen	
Virenscanner am Computer ausschalten	
MAC-Adressenfilter am vorhandenen Router ausschalten	

Notwendige Daten	Kommentar
Netzwerk SSID	
IP – Gateway	
IP – DNS-Server	
DHCP Range	
Subnetzmaske	
IP – Internetzugang	
IP – Timeserver (wenn vorhanden)	
Passwort – Internetzugang	
Passwort – WLAN	
IPs von vorhandenen Servern (wenn vorhanden)	
IP – Watchdog (wenn vorhanden)	
IP – Log-Server (wenn vorhanden)	
IP – virtuelle DMZ (wenn vorhanden)	

